フィッシング対策協議会
平成19年度第2回技術・制度検討ワーキンググループ
2007年9月20日 後日配布版

# 正しいフィッシング対策について

独立行政法人産業技術総合研究所
情報セキュリティ研究センター
高木 浩光
http://staff.aist.go.jp/takagi.hiromitsu/

## 対策の方向性

- Webの正しい利用方法の理解の普及
  - 啓発活動
  - パソコン、OSの取扱説明書への記載
  - 学校教育のカリキュラムへの盛り込み
- 技術的欠陥（脆弱性）の排除
  - ブラウザの脆弱性の修正
  - Webサイト側の脆弱性の修正
    - クロスサイトスクリプティング脆弱性の排除
- 技術的解決策
  - EV-SSL
  - ツールバーによる利用者補助
  - パスワード自動入力ツール
  - ログイン認証方式の改善

## 杜撰な啓発活動

- インチキ解説の氾濫
  - 経済産業省、フィッシング対策協議会、JPCERT/CC、マイクロソフト、アンチウイルスソフトベンダ、都市銀行の一部
  - 広告会社丸投げ、素人に書かせ、誰もチェックしない
- 「専門家」も実は理解していない
  - 誤った解説の例
    - 「アドレスバーも偽装されるのであてにならない」
    - 「すべてのページでサーバ証明書の内容を確認するなんて無理だ」

中略

# 適切な解説の例

- 三井住友銀行
  「簡単! やさしいセキュリティ教室」
  http://www.smbc.co.jp/kojin/security/school/index.html

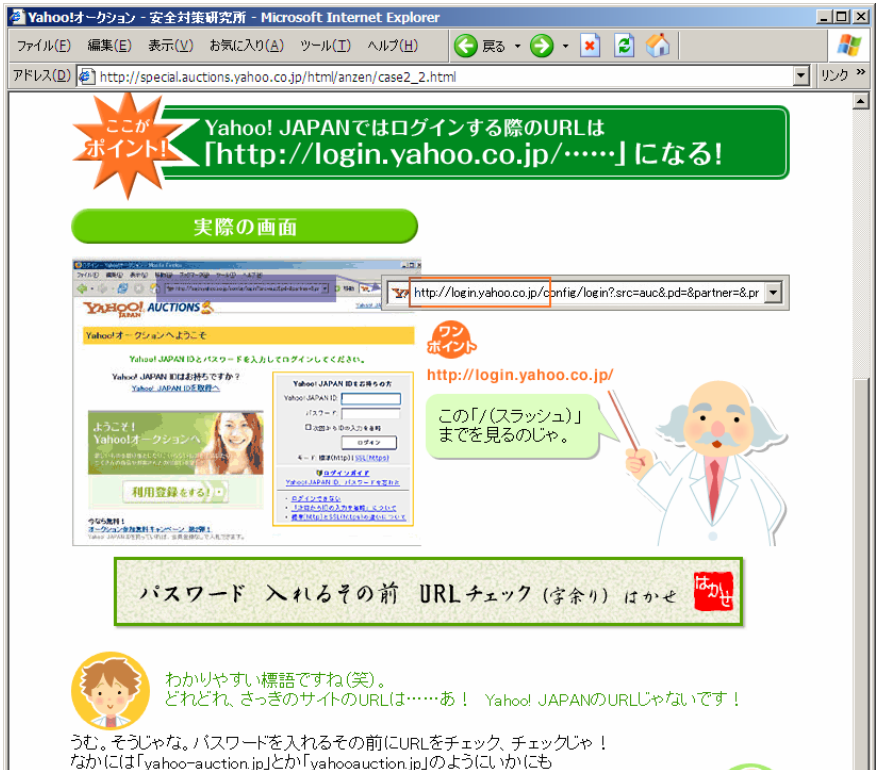
中略

# 我々の取組：啓発コンテンツの制作

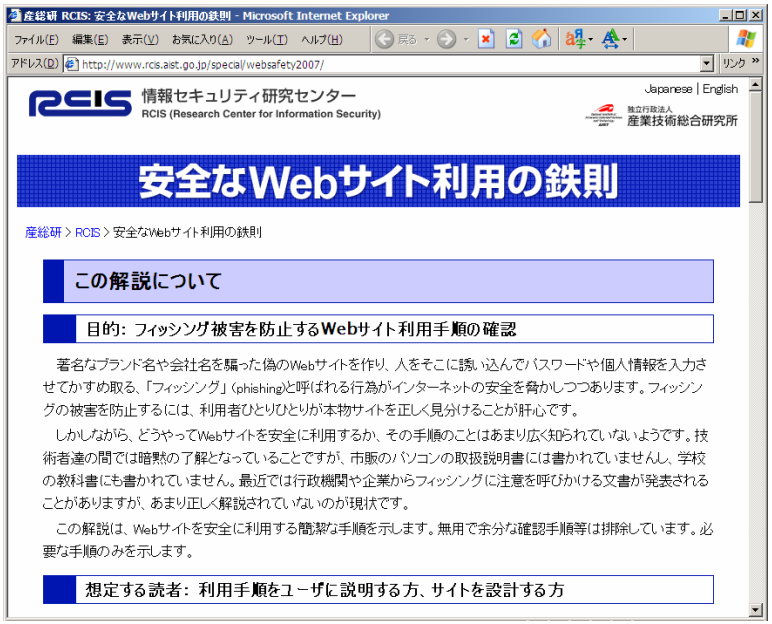
- 産総研とヤフーの共同研究の一環

- ヤフー側
  - 「Yahoo!オークション 安全対策研究所」
    http://special.auctions.yahoo.co.jp/html/anzen/
    - フィッシングに騙されないための、利用者向けの注意点を、Yahoo!オークションを実例として解説（監修を担当）
- 産総研側
  - 「安全なWebサイト利用の鉄則」
    http://www.rcis.aist.go.jp/special/websafety2007/
    - フィッシング被害を防止するWebサイト利用手順の考え方を一般論として
    - 利用マニュアル制作者、サイト設計者向けに解説

# ヤフー側




# 産総研側




# 「鉄則」の要点

- 初めて訪れたサイトの場合
  - サイト運営者のことを知っている場合
    - その運営者のドメイン名を既に知っている場合
      - アドレスバーのドメイン名を確認する
    - その運営者のドメイン名をまだ知らない場合
      - SSLのサーバ証明書の内容を確認する
  - サイト運営者のことをまだ知らない場合
    - (信用できる運営者か見極める)
- 再度訪れたサイトの場合
  - アドレスバーのドメイン名を確認する

# 基本手順

- アドレスバーに表示されたURLのドメイン名を目視確認する

http://list3.auctions.yahoo.co.jp/jp/23336-cate**本物**html
「ドメイン名」

http://www.yahoo.co.jp.auction.jp/23336-cate**偽物**ml
「ドメイン名」

http://list3.auctions.jp/yahoo.co.jp/23336-cat**偽物**ml
「ドメイン名」

右端
http://.....yahoo.co.jp/.....
最初の「/」

# アドレスバーの役割

- 昔々、元々は入力できない場所だった
  - 1994年6月の改良「NCSA Mosaic 2.0alpha5」の際に、アドレスバーに直接URLを書き込めるようになった
- 「今見ているページのURLがどこか」を表示する機能
  - 1994年6月まではそれだけの機能だった
  - それが本来の機能

- その後、アドレスバーの役割がおろそかにされるようになった
  - 例: 携帯電話のWebブラウザ

- フィッシング詐欺の多発で、重要性が再認識

# 「不審なメール」に注意?

- 警察庁の呼びかけ
  - 「個人情報やカードの情報などを問い合わせる不審な電子メールやホームページには注意が必要です」
    http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm
  - 「不審なメール」と見抜けるのか?
  - 「個人情報やカード情報を求めるメール = 不審なメール」という意味か?

- 銀行やカード会社の対応
  - 「当社からお客様に暗証番号やカード番号をお尋ねすることはありません」とする告知が流行した
  - それは本当か?

# 正規の誘導メール

差出人: "三井住友銀行 電子メールお知らせサービス" <SMBC_service@dn.smbc.co.jp> 宛先:
件名: 【三井住友銀行】振込入金のお知らせ 日時: Mon, 25 Apr 2005 10:01:07 +0900 (GMT+09:00)

【金融機関等を装う電子メールにご注意ください】
電子メールに記載されているURLおよびそのリンク先は必ずご確認ください。
くわしくは、弊行のホームページをご覧ください。

いつも三井住友銀行をご利用いただきありがとうございます

タカギ ヒロミツさま

以下の振込入金がございましたのでお知らせいたします。

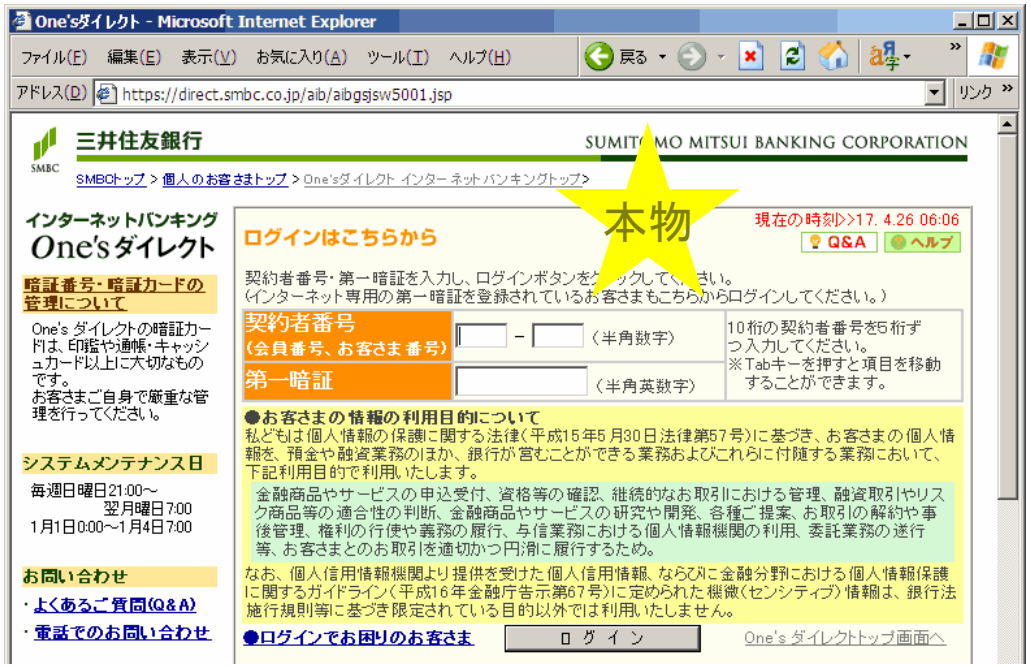
入金口座 : 支店 普通(総合) 口座番号
入金日 : 平成17年04月25日
金額 : 4,442円
内容 : 振込

平成17年04月25日09時26分現在(配信番号: -0010)

※振込、残高照会、定期預金・外貨預金・投資信託などのお取り引きは
以下のアドレスから、One's ダイレクト(インターネットバンキング)に
ログインしてご利用ください。

→ http://direct.smbc.co.jp/

本物




「ログインしてください」=「暗証番号を入力してください」

# 手口の巧妙化

- 初期段階――緊急事態を装って入力させる
  - 「あなたの口座に問題が生じました」

- 手口の巧妙化――正規のメールの模倣
  - 平常どおりのメールで、リンク先だけが偽サイトに差し替えられている
    - 警戒している者にも「怪しいメール」とは気付けない
  - 既にそのような手口が横行している

# 不安ビジネスに踊らされない

- 「偽装されるからアドレスバーを見ちゃダメだ」という人がいるが
  - 「だからフィッシング対策ソフトを買え」と?
- 「Windows Updateできない人がいるから」
  - そうかもしれないが、だからどうすればよい?
- 「証明書を確認しろなんて無理だ」
  - 確認する必要などない
  - 過大なリテラシーを仮定して否定し、リテラシーではどうにもならないと主張する人達がいる
- そして誰もリテラシーを説かない

# 安全なWeb利用の鉄則

- 既に知っているサイトを利用する場合
  - アクセスした後、重要な情報を入力する前に以下を確認する
    - アドレスバーに表示されたURLのドメイン名を目視確認する
    - 錠前アイコンの存在を確認する（内容は見なくてよい）
  - その前に
    - SSLの証明書異常警告が出ていたら「いいえ」を押す
- 初めて訪れたサイトを利用する場合
  - https:// の画面を探して、錠前アイコンをダブルクリックして、サーバ証明書の内容を確認する

# アドレスバーを目視確認する

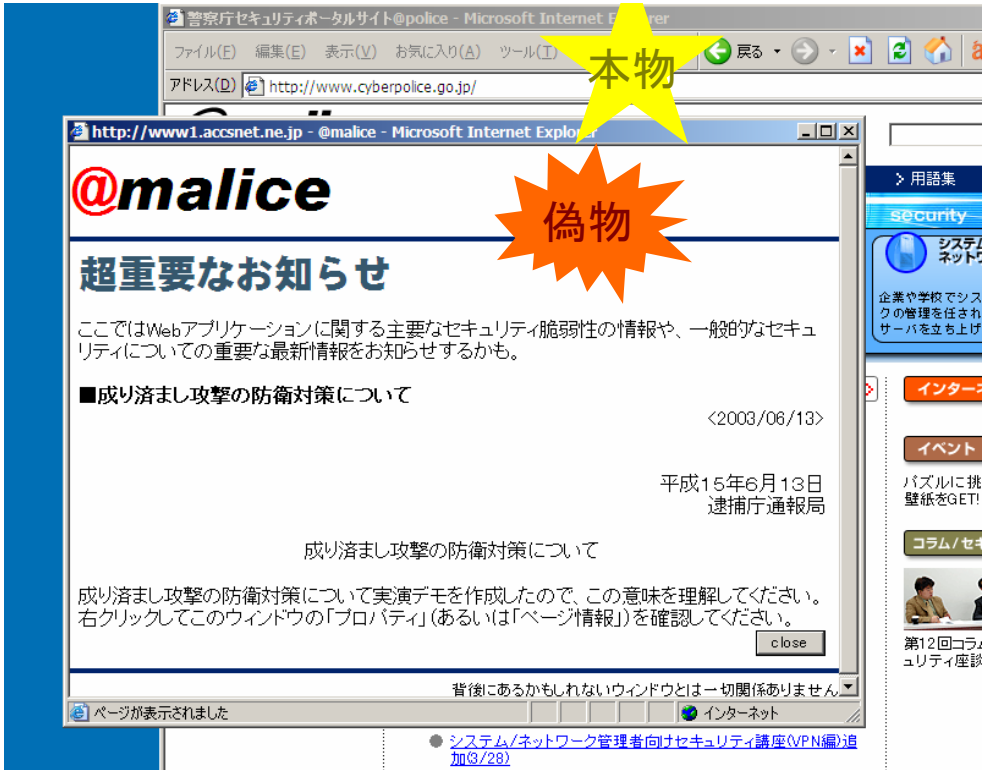
- アドレスバーに表示されたURLを目視確認する
  - ドメイン名さえ確認すればよい（URL全部は確認不要）
  - 自分が信頼しているサイトのドメイン名は暗記しておく

- ウィンドウにアドレスバーが出ていない場合
  - 偽サイトかもしれないと判断して入力を避ける

# Pop-Upウィンドウによる手口

- 本物サイトのウィンドウの上に重ねて、偽のログイン用ウィンドウを開き、そのアドレスバーを隠す

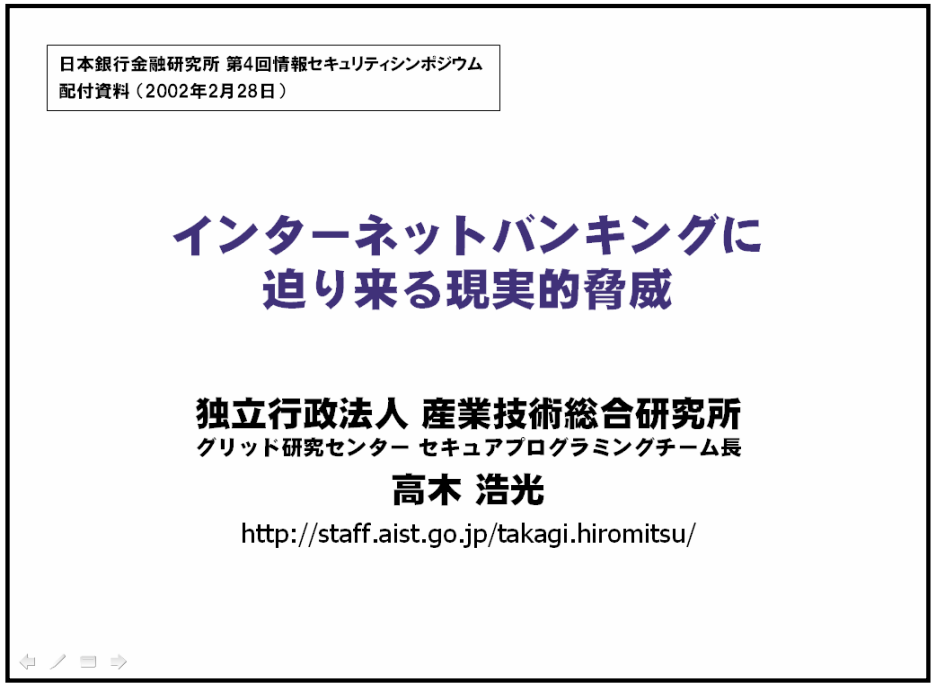
- なぜそんなことができるか
  - 被害者が偽サイトに誘導されてジャンプすると、
  - 偽サイトにはJavaScriptが埋め込まれていて、
  - JavaScriptによりポップアップウィンドウが開かれ、そこには偽ページが表示され、
  - JavaScriptにより元のウィンドウが本物サイトへジャンプさせられる




# アドレスバーを隠す本物サイト

- 本物サイトにもアドレスバーがないのですが……
  - 偽サイトと見分けがつかないようなサイトは使わない

- それでは困るのですが……
  - アドレスバーを隠すようなサイトはセキュリティ意識が低いと考えられ、そのようなサイトは他にもセキュリティの欠陥を抱えている可能性があると考えられるという理由から、いずれにせよそのサイトは使わない方が懸命……と判断することができる




2002年2月の日本銀行金融研究所での講演資料より

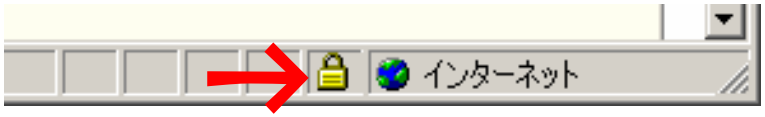
中略

## その後

- 2004年11月ごろ、大半の大手銀行がアドレスバーを隠すのをやめた
- サイト運営者側の責任
  - 利用者が本物確認しやすいサイト設計を

## 錠前アイコンの存在を確認する

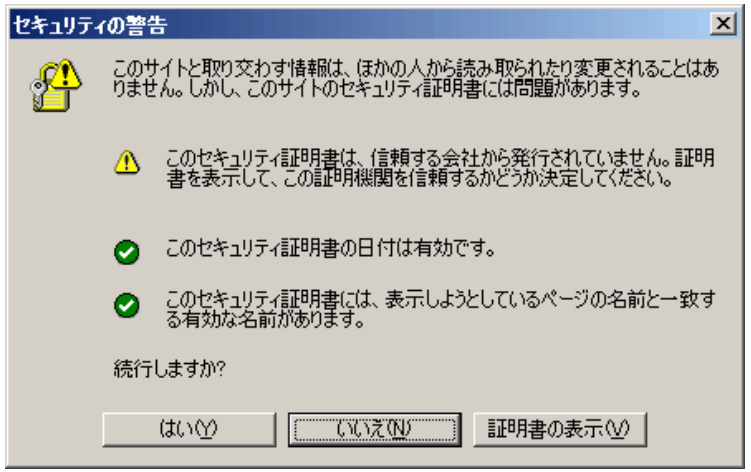
- 個人情報やパスワードなど重要な情報を入力する画面では、SSLによる暗号化通信が提供されている
  - SSLが使われていないならば入力しない
  - ステータスバーが隠されているなら使わない




- 注意!!
  - 偽サイトが、偽サイト用の錠前アイコンを出していることもある
  - アドレスバーの確認と両方を確認する必要がある

## この警告が出たら危ない

- 偽のサーバ証明書で運用されているSSLサイトの可能性をブラウザが自動判別して指摘している



# 警告を無視させるサイトは本物か?

- 本物サイトが次の指示をしていることがある
  - 警告が出ても「はい」を押すように指示
  - 警告が出ないようにするため証明書をインストールするように指示
  - 商用サイトでは少ないが、官庁、自治体、大学サイトがこうした指示をしている
- Phishingサイトがそうした指示をするようになるおそれ
  - 消費者としては、こうした指示は一律に無視する

# 紛らわしいドメイン名の問題

- 最近の銀行の告知
  - 「当行のドメイン名は『〇〇bank.co.jp』です」
- たとえば、「i」と「l」の見分けができるか
  - 実際にあった事例

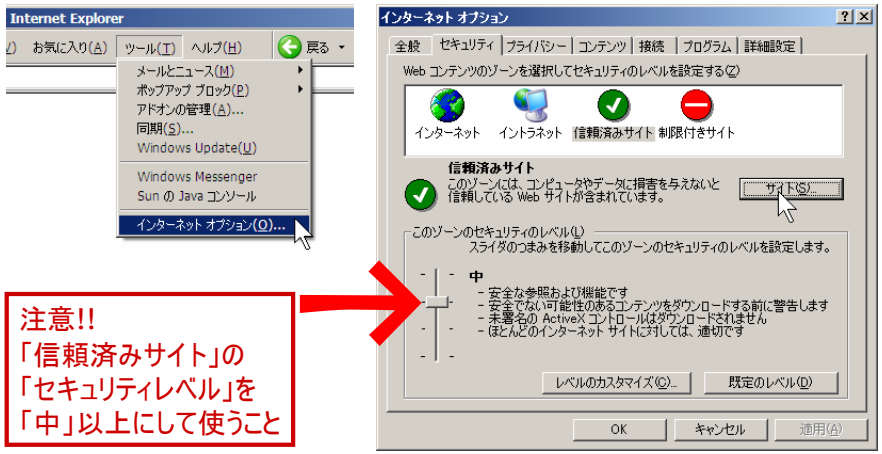
http://www.paypal.com/ 本物

http://www.paypai.com/ 偽物

- 「覚えておく」「見分ける」なんて無理?

# 機械的に見分ける方法

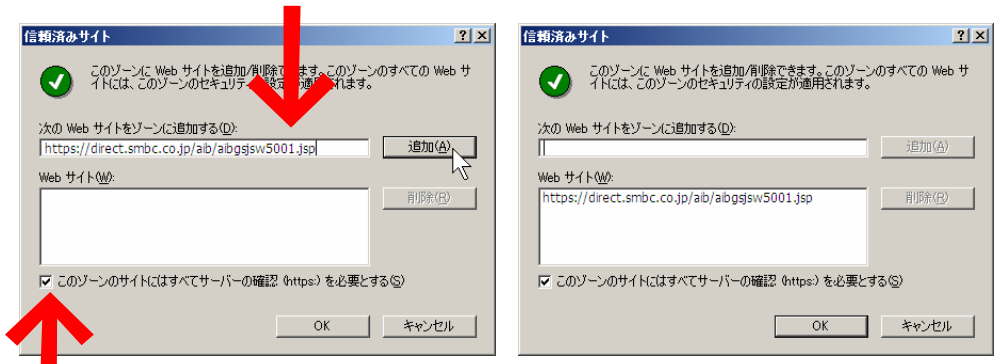
- Internet Explorer の「信頼済みサイト」の機能を使う




注意!!
「信頼済みサイト」の
「セキュリティレベル」を
「中」以上にして使うこと

# 確認したサイトを登録する

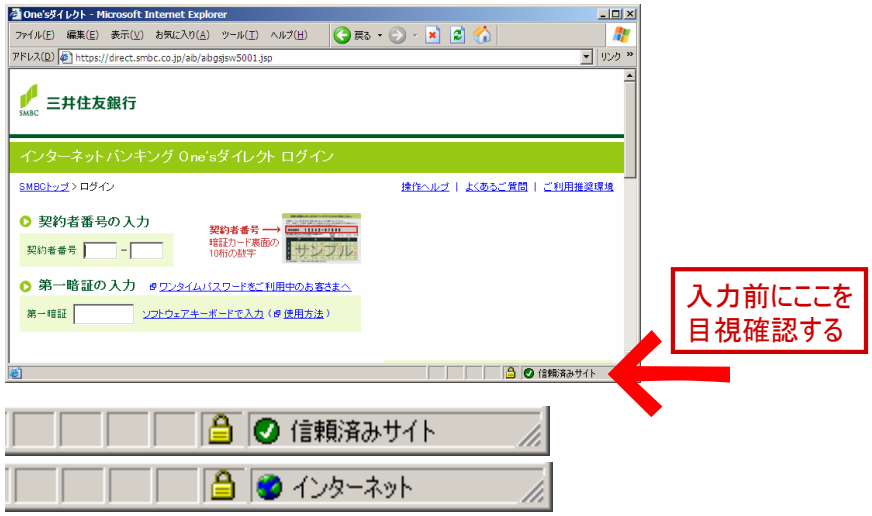
- 本物サイトだと確認できたページのURL（https:// の）を登録する




このチェックは外さない

# 二度目以降は簡単に確認できる

- 一度慎重に本物だと確認したサイトは、「信頼済みサイト」に登録しておけば、簡単に確認できる




# 初めて訪れたサイトの場合

- 知らない会社や団体のサイトを訪れた場合
  - そもそもその会社を信用してよいか
    - やっていることがすべて詐欺だったりしないか?
- 知っている会社や団体のサイトを訪れたつもりの場合
  - 本当にその会社のサイトなのか
  - サーバ証明書の内容を見て運営者の名前と住所を確認する
    - サーバ証明書のいわゆる「実在証明機能」
    - 会社名よりドメイン名の方が有名である場合には、これを確認する必要がない（ドメイン名を慎重に確認すれば）

# これで安全か?

- 次の可能性があるので必ず安全とは言えない
  - アドレスバー偽装、錠前アイコン偽装の手口が使われている可能性
  - クロスサイトスクリプティング攻撃により、本物サイトの画面上に、偽ページが埋め込まれている可能性
  - 本物サイトが侵入されてコンテンツが偽ページに改ざんされている可能性
  - Pharming（ファーミング）の手口によって、自分のパソコンが既に汚染されている（設定を変更されている等）可能性
- どうしようもないのか?

# 責任分界点を明確に

- アドレスバー偽装、錠前アイコン偽装
  - Webブラウザベンダーの責任
    - アドレスバーや錠前アイコンを正しく確認できないようなものは、ブラウザとして欠陥があるという共通認識がある
    - ブラウザの脆弱性として発見されしだい修正されている
- クロスサイトスクリプティング攻撃
  - Webサイト運営者の責任
    - Webアプリケーションの脆弱性であり、修正すべきもの
- 本物サイトが偽ページに改ざん
  - Webサイト運営者の責任
    - そもそもあってはならないこと
- Pharming（ファーミング）の手口
  - 消費者の責任
    - スパイウェア等に感染するようなミス操作をしては、どうしようもない

## 事業者のとるべき対策

- Webサイトの構成のあるべき姿
  - アドレスバーやステータスバーを隠さない
  - 入力ページを https:// にする
  - 正規のサーバ証明書を購入してSSLを運用する
  - サービス提供者が保有するドメイン名を使う
  - まぎらわしくないドメイン名を使う
  - サイトからクロスサイトスクリプティング脆弱性を排除する
- メール配信のあるべき姿
  - HTMLメールを送らない
  - デジタル署名のないメールを送らない

## クロスサイトスクリプティング

- クロスサイトスクリプティング（Cross-Site Scripting）脆弱性（「XSS脆弱性」）とは
  - CERT/CCが2000年2月に勧告
    - CERT Advisory CA-2000-02 “Malicious HTML Tags Embedded in Client Web Requests”
  - Cookie漏えい、セッションハイジャック攻撃の危険があるとして国内では比較的よく知れ渡り対策が進んだ
- もう一つの脅威
  - 本物サイトの画面上に偽ページを差し込まれる
    - サーバ内の記憶データが改ざんされるわけではない
    - 外部からの入力を差し込んで表示する動的なページで、適切な作り方をしていないと、JavaScriptをページ内に差し込まれる
    - 悪意あるサイトからジャンプしてきた場合に起きる

## 狭義のXSSと広義のXSS

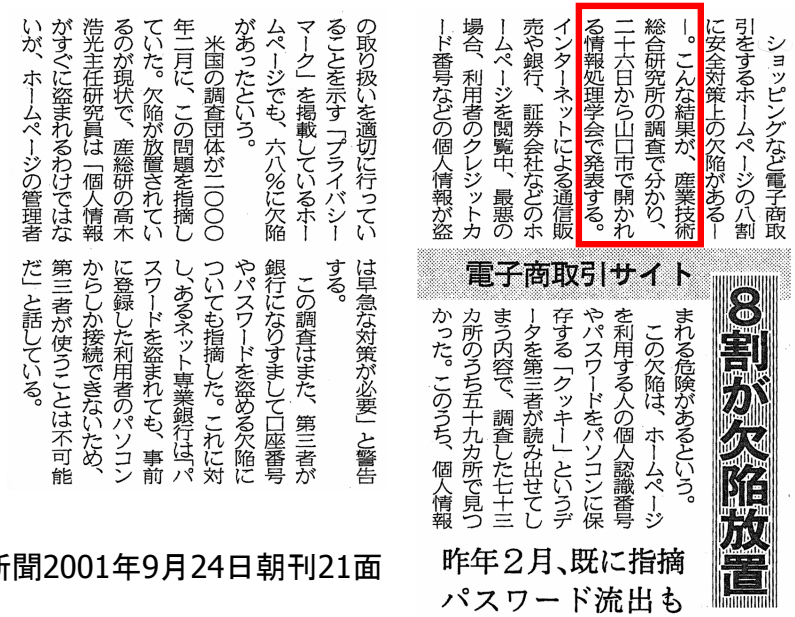
- 狭義のXSS
  - 外部サイト（攻撃者のページ）からのリンクを辿ったときにHTML断片を差し込まれる
  - ページの差し替えは一時的に発生する
  - あらゆるサイトにおいてあり得る
- 広義のXSS
  - 攻撃者がHTML断片（特にスクリプト）を書き込む
  - ページの差し替えは永続的に発生する
  - 掲示板、Webメール等の誰でも書き込みが可能なサービスにおいて起こり得る

## Yahoo! JAPANの事例

- 2005年11月に発生した日本語phishing
  - Yahoo!メール（Webメールサービス）に届いたHTML形式のphishingメール
  - Yahoo!メールのXSS脆弱性を突いて、yahoo.co.jpドメインの画面上に偽コンテンツを表示させていた
  - 広義のXSSの事例

中略

# 狭義のXSS



8割が欠陥放置

電子商取引サイト

昨年2月、既に指摘
パスワード流出も

ショッピングなど電子商取引をするホームページの八割に安全対策上の欠陥があるー。こんな結果が、産業技術総合研究所の調査で分かり、二十六日から山口市で開かれる情報処理学会で発表する。

インターネットによる通信販売や銀行、証券会社などのホームページを閲覧中、最悪の場合、利用者のクレジットカード番号などの個人情報が盗まれる危険があるという。

この欠陥は、ホームページを利用する人の個人認識番号やパスワードをパソコンに保存する「クッキー」というデータを第三者が読み出せてしまう内容で、調査した七十三カ所のうち五十九カ所で見つかった。このうち、個人情報の取り扱いを適切に行っていることを示す「プライバシーマーク」を掲載しているホームページでも、六八%に欠陥があったという。

米国の調査団体が二〇〇〇年二月に、この問題を指摘していた。欠陥が放置されているのが現状で、産総研の高木浩光主任研究員は「個人情報がすぐに盗まれるわけではないが、ホームページの管理者は早急な対策が必要」と警告する。

この調査はまた、第三者が銀行になりすまして口座番号やパスワードを盗める欠陥についても指摘した。これに対し、あるネット専業銀行は、パスワードを盗まれても、事前に登録した利用者のパソコンからしか接続できないため、第三者が使うことは不可能だ」と話している。

日経新聞2001年9月24日朝刊21面

中略

# 技術による解決策

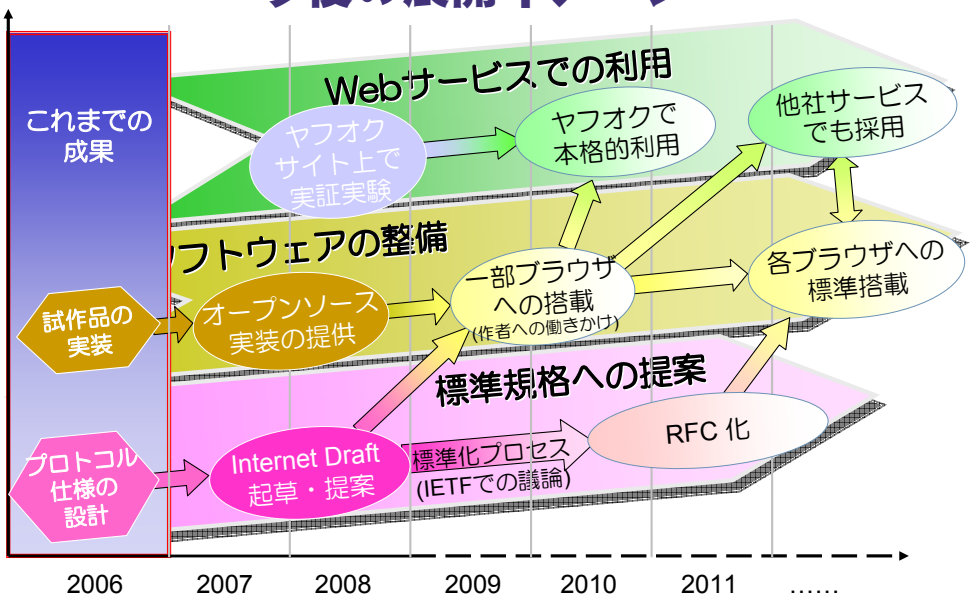
- EV-SSL
  - ホワイトリスト
    サイト運営者の信頼性を専門機関が審査認定する
    - 欠点：正当なサイトのすべてが利用できるわけではない
- ツールバーによる利用者補助
  - ブラックリスト、特徴検出（IE 7、Firefox 2）
  - ドメイン名の視認性向上（各種Firefoxアドオン等）
  - 信頼するドメインの登録・確認ツール（「Petname Tool」）
- パスワード自動入力ツール
  - 「PwdHash」(Stanford)、「Passpet」(UCB)等
- ログイン認証方式の改善
  - 産総研－ヤフー共同研究の事例

中略

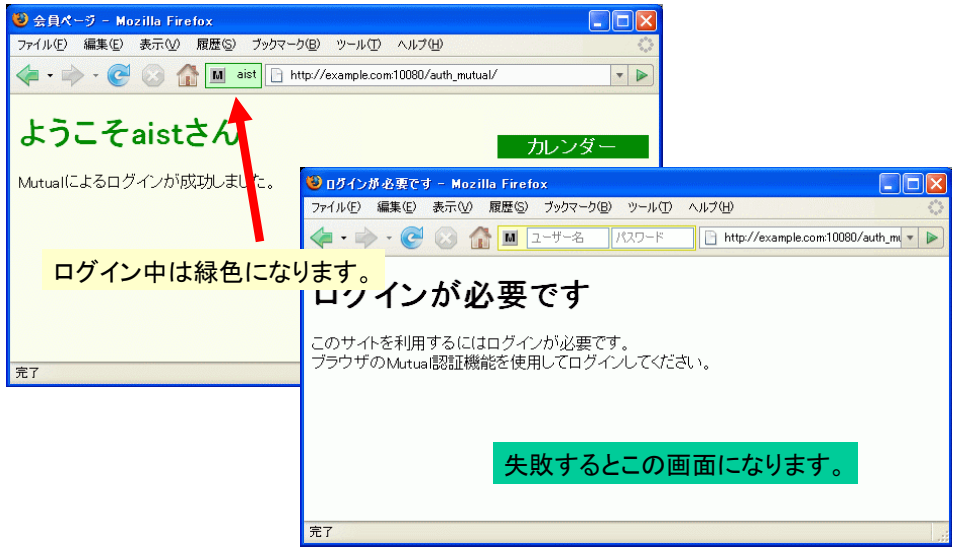
# 産総研とヤフーが提案する新認証プロトコル

- 長期的展望に立った抜本的解決策
- HTTP Auth（「Basic認証」等）の拡張「Mutual Auth」
  - Basic, Digest, Mutual
- フォーム認証はもうやめよう
  - Webアプリケーションの脆弱性も同時に減らせる
  - Webアプリケーションのログイン機能実装が容易になる

# これまでの成果と今後の展開イメージ




# 開発した技術



## 技術的解決の必要性と前提

- 被害に遭うケース
  - ドメイン名の確認を怠ってしまった場合
  - ドメイン名を覚えていられない場合
  - 紛らわしいドメイン名の偽サイトが現れた場合
    - http://www.yafoo.jp/
    - http://www.yahoo.co.jp.auction.jp/23336-category/
    - http://list3.auctions.jp/yahoo.co.jp/23336-category.html

偽物

- 前提
  - 経験豊富なユーザでも、うっかり見逃してしまうことがある
  - 既にパスワードを登録済みのサイトを利用する場合
  - 通信路での盗聴よりも、偽サイトによるフィッシングの方が、現実的に大きな脅威になっている

## 技術的なポイント

- ユーザインターフェイスの改良
- 認証方式として PAKE を採用
- HTTP Authentication を自然に拡張して設計
- HTTPS との組み合わせに配慮
  - 新たに生じた問題を解決
- ブラウザ側に事前の設定が不要で、どの端末でも利用できる（ブラウザがこのプロトコルを標準搭載した後には）

⇒個人情報入力時の新しいリテラシの提案

緑色になっていれば入力してもOK

## 本技術の目標

- ユーザが偽サイトに誤ってログインしようとしても
  - パスワードが詐取されない
  - ユーザが自分が期待しているサイトと通信していないことを検知できる

ような認証機能を実現する。

⇒ PAKE と呼ばれる暗号技術を応用

PAKE (Password Authenticated Key Exchange)

略